AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently amended) A content management method for [[a]] managing content data ~~storage~~ provided ~~with a plurality of content storing means~~ to user equipment, comprising the steps of:

storing a content key encrypted with a first storage key, ~~in a first content storing means, and storing along with said content key encrypted with the first storage key a~~ content data encrypted with the content key, and a second storage key in the user equipment;

sending the encrypted content key and the second storage key to a key management unit;

at the key management unit, decrypting the encrypted content key ~~with~~ using the first storage key, the first storage key being stored in the key management unit; and

encrypting the decrypted content key ~~obtained by the above decryption with a newly generated~~ using the second storage key[[,]];

~~storing~~ sending the content key encrypted with the second storage key along with the encrypted content ~~in a second content storing means~~ to the user equipment; and

~~re-encrypting~~ at the user equipment, decrypting the encrypted content key using ~~a user~~ the second storage key and ~~storing~~ decrypting the content data ~~to an external storage medium~~ using the decrypted content key.

2. (Original) The method as set forth in Claim 1, wherein the second storage key is generated based on a random number.

3. (Currently amended) The method as set forth in Claim 1, wherein the decrypted content key ~~obtained by the decryption~~ is encrypted with identification information of the ~~second content storing means~~ user equipment and stored into the ~~second content storing means~~ user equipment.

4. (Currently amended) The method as set forth in Claim 1, wherein the content key is encrypted, in the ~~first content storing means~~ user equipment, with the first storage key and identification information of the ~~first content storing means~~ user equipment, and the content key stored in the ~~first content storing means~~ user equipment is decrypted with the first storage key and the identification information of the ~~first content storing means~~ user equipment.

5. (Currently amended) The method as set forth in Claim 1, wherein the second storage key is generated by a decrypted key generating means provided in the ~~data storage~~ user equipment.

6. (Currently amended) The method as set forth in Claim 5, wherein the second storage key is encrypted with a public key for [[a]] the key management unit for management of the storage keys to generate a third storage key and the third storage key is stored into the ~~second content storing means~~ user equipment.

7. (Currently amended) The method as set forth in Claim 6, wherein the ~~data storage~~ user equipment deletes the second storage key depending upon whether the third storage key has been stored in the ~~second content storing means~~ user equipment.

8. (Currently amended) The method as set forth in Claim 7, wherein when decrypting the content key stored in the ~~second content storing means~~ user equipment, the ~~data storage~~ user equipment sends the third storage key to the key management unit; and the key management unit generates [[a]] the second storage key based on the third storage key while accounting the data service following a predetermined procedure.

9. (Currently amended) The method as set forth in Claim 1, wherein the second storage key is generated by a storage key generating means provided in the key management unit which manages the storage keys; and the key management unit has stored therein the second storage key and ~~the~~ identification information of the ~~second content storing means~~ user equipment in which the content key encrypted with the above generated second storage key is stored.

10. (Original) The method as set forth in Claim 9, wherein upon the generation of the second storage key, the key management unit accounts the data service following the predetermined procedure.

11. (Currently amended) The method as set forth in Claim 9, wherein the key management unit encrypts the second storage key with the management key to generate a third storage key, and sends the third storage key to the ~~data storage~~ user equipment; and the ~~data storage~~ user equipment stores the received third storage key ~~into the second content storing means~~.

12. (Currently amended) The method as set forth in Claim 11, wherein the ~~data storage~~ user equipment deletes the second storage key depending upon whether the third storage key has been stored ~~in the second content storing means~~.

13. (Currently amended) The method as set forth in Claim 12, wherein the key management unit has stored therein the identification information of the ~~second content storing means~~ user equipment in which the content key encrypted with the second storage key is stored; the ~~data storage~~ user equipment sends, when decrypting the content key stored in the ~~second content storing means~~ user equipment, the identification information of the ~~second content storing means~~ user equipment to the key management unit; and the key management unit generates [[a]] the second storage key based on the result of comparison between ~~the~~ identification information of the ~~second content storing means~~ user equipment, ~~send~~ sent from the ~~data storage~~ user equipment, and the identification information of the ~~second content storing means~~ user equipment, held in the key management unit itself, while accounting the data service following the predetermined procedure.

14. (Currently amended) The method as set forth in Claim 1, wherein the ~~second content storing means~~ user equipment has stored therein ~~the~~ identification information of the ~~data storage~~ user equipment.

15. (Currently amended) The method as set forth in Claim 14, wherein the ~~data storage~~ user equipment starts decrypting the content key stored in the ~~second content storing means~~ user equipment depending upon the result of an inspection of the identification information of the ~~data storage~~ user equipment, stored in the ~~second content storing means~~ user equipment.

16. (Currently amended) The method as set forth in Claim 1, wherein the decrypted content key supplied from the ~~second content storing means~~ user equipment has added thereto information that the content key ~~is a one~~ has been obtained by restoration.

17. (Currently amended) The method as set forth in Claim 16, wherein when moving the content key having added thereto the information that the content key ~~is a restored one~~ has been obtained by restoration, the ~~data storage~~ user equipment performs ~~makes~~ an error process based on the result of comparison between the content key and [[a]] another content key stored in a destination to which the content key is to be moved.

18. (Original) The method as set forth in Claim 1, wherein the content key has added thereto frequency information which limits the number of times the content key can be used.

19. (Currently amended) The method as set forth in Claim 1, ~~wherein~~ further comprising storing the content key ~~stored in the first content storing means is stored~~ encrypted with the second storage key in a first storage of the user equipment along with ~~the~~ identification information of the ~~first content storing means~~ first storage; storing the content key that is stored in the first storage, and the identification information of the first storage, into ~~the second content storing means~~ a second storage of the user equipment; ~~the identification information stored in the second content storing means is stored into the data storage when the content key stored in the second content storing means is decrypted~~; and ~~the data storage makes~~ performing, when a request is made to decrypt the content key in the ~~first content storing means~~ first storage, an error process based on the result of comparison between the identification information of the ~~first content storing means in consideration~~ first storage and the identification information of the ~~second content storing means~~ second storage.

20. (Currently amended) A content ~~storage~~ management system for managing content data, comprising:

a first ~~content~~ storing means having stored therein a content key encrypted with a first storage key, ~~and a~~ content data encrypted with the content key, and a second storage key;

a first sending means for sending the encrypted content key and the second storage key to a key management unit;

a first decrypting means, in the key management unit, for decrypting the encrypted content key ~~data~~ using the first storage key, the first storage key being stored in the key management unit;

an encrypting means for encrypting the decrypted content key ~~data~~ using the second storage key; and

~~means for generating a first storage key;~~

~~means for generating a second storage key;~~

~~a second content storing means for storing an encrypted content key obtained by encrypting, in the encrypting means, the content key obtained by decryption with the first storage key in the decrypting means, using the second storage key generated by the second storage key generating means, and the encrypted content; and~~

~~means for storing the storage keys;~~

a second decrypting means for ~~re-encrypting~~ decrypting the encrypted content key using ~~a user~~ the second storage key and ~~storing~~ decrypting the content data ~~to an external storage medium~~ using the decrypted content key.

21. (Currently amended) The system as set forth in Claim 20, ~~wherein the~~ further comprising storage key ~~storing~~ generating means ~~generates~~ for generating the second storage key by means of a random number generator.

22. (Currently amended) The system as set forth in Claim 20, wherein ~~a content key obtained by encrypting, in the encrypting means,~~ the encrypting means encrypts the decrypted content key ~~obtained by the decryption in the decrypting means,~~ with ~~the first storage key and~~ identification information of ~~the~~ a second ~~content~~ storing means~~, is stored in the second content storing means~~.

23. (Currently amended) The system as set forth in Claim 20, wherein the content key is encrypted, in the first ~~content~~ storing means, with the first storage key and identification information of the first ~~content~~ storing means; and the content key stored in the first ~~content~~ storing means is decrypted with the first storage key and the identification information of the first ~~content~~ storing means.

24. (Currently amended) The system as set forth in Claim 20, wherein the first ~~content~~ storing means, first decrypting means, and encrypting means~~, second content storing means, storage key storing means and storage key generating means~~ form together a data storage[[;]], and ~~further comprising a~~ wherein the key management unit ~~which~~ manages the second storage ~~keys~~ key of the data storage.

25. (Currently amended) The system as set forth in Claim 24, wherein the data storage is a data receiver which receives a content data encrypted and sent from a data transmitter.

26. (Currently amended) The system as set forth in Claim 24, further comprising means for storing ~~the~~ a public key of the key management unit; and wherein the second content storing means has stored therein the second storage key along with a third storage key obtained by encrypting the second storage key with the public key.

27. (Currently amended) The system as set forth in Claim 26, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the second ~~content~~ storing means.

28. (Currently amended) The system as set forth in Claim 27, wherein, when decrypting the content key stored in the second ~~content~~ storing means, the data storage sends the third storage key to the key management unit; and the key management unit sends [[a]] the second storage key generated based on the third storage key to ~~the~~ a data transmitter while accounting the data service following a predetermined procedure.

29. (Currently amended) The system as set forth in Claim 24, wherein the second ~~content~~ storing means has stored therein ~~the~~ identification information of the data storage.

30. (Currently amended) The system as set forth in Claim 29, wherein the data storage starts decrypting the content key stored in the second ~~content~~ storing means depending on the result of inspection of the identification information of the data storage, stored in the second ~~content~~ storing means.

31. (Currently amended) The system as set forth in Claim 20, wherein the first ~~content~~ storing means, first decrypting means, and encrypting means~~, second content storing means and storage key storing means~~ form together a data storage; and comprising ~~the~~ a storage key generating means, ~~and further a~~ wherein the key management unit ~~which~~ manages the second storage ~~keys~~ key of the data storage.

32. (Currently amended) The system as set forth in Claim 31, wherein the data storage is a data receiver which receives a content data encrypted and sent from a data transmitter.

33. (Currently amended) The system as set forth in Claim 31, wherein the key management unit comprises an identification information storing means in which ~~the storage key generated by the key management unit and the~~ identification information of the ~~content~~ first storing means ~~in which the content key encrypted with the generated storage key~~ is stored.

34. (Currently amended) The system as set forth in Claim 31, wherein the key management unit accounts the data service following the predetermined procedure depending upon ~~the~~ a generation of the second storage key.

35. (Currently amended) The system as set forth in Claim 31, wherein the key management unit comprises means for storing storage keys; the key management unit

generates a third storage key by ~~decrypting~~ encrypting the second storage key with ~~the storage~~ a management key and sends [[it]] the third storage key to the data storage; and the data storage stores the third storage key into the second ~~content~~ storing means.

36. (Currently amended) The system as set forth in Claim 35, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored ~~into~~ in the second ~~content~~ storing means.

37. (Currently amended) The system as set forth in Claim 36, wherein the key management unit comprises means for storing the second storage key and ~~the~~ identification information of the second ~~content~~ storing means in which the content key encrypted with the second storage key is stored; the key management unit accounts, when the data storage decrypts the content key, the data service following the predetermined procedure based on the result of comparison between the identification information of the second ~~content~~ storing means, sent from the data storage, and ~~the~~ identification information stored in ~~the~~ an identification information storing means.

38. (Currently amended) The system as set forth in Claim 31, wherein the second ~~content~~ storing means has stored therein ~~the~~ identification information of the data storage.

39. (Currently amended) The system as set forth in Claim 38, wherein the data storage starts decrypting the content key stored in the second ~~content~~ storing means.

40. (Currently amended) The system as set forth in Claim 20, wherein the content key obtained by decryption from the second ~~content~~ storing means has added thereto information that the content key ~~is a one~~ has been obtained by restoration, as requirement information.

41. (Original) The system as set forth in Claim 20, wherein the content key has added thereto frequency information which limits the number of times the content key can be used.